PCT / IB04/50358

Europäisches Patentamt | European Patent Office | Office européen des brevets

BEST AVAILABLE COPY

REC'D 02 APR 2004
WIPO PCT

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03100837.8

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03100837.8
Demande no:

Anmeldetag:
Date of filing: 31.03.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Erteilungsverfahren zum Erteilen einer Veränderungsberechtigung

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/ Classification internationale des brevets:

G07F7/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT SE SI SK TR LI

Erteilungsverfahren zum Erteilen einer Veränderungsberechtigung

Die Erfindung bezieht sich auf ein Erteilungsverfahren, um einer Veränderungseinrichtung eine Veränderungsberechtigung zum Verändern einer Applikation in einem Datenträger zu erteilen.

Die Erfindung bezieht sich weiters auf einen Datenträger zum Abarbeiten zumindest einer Applikation.

Die Erfindung bezieht sich weiters auf eine Veränderungseinrichtung zum Verändern einer Applikation in dem Datenträger.

Ein solcher Datenträger ist in dem Dokument EP 0 935 214 A offenbart, wobei der Datenträger durch eine Chipkarte gebildet ist. Rechnermittel des Datenträgers sind zum Abarbeiten mehrerer Applikationen beziehungsweise Softwareprogramme ausgebildet. Der bekannte Datenträger kann beispielsweise eine Bank-Applikation abarbeiten, bei deren Abarbeitung Geldbeträge bei einem Bankautomaten auf den Datenträger aufgeladen und in einem Geschäft zur Bezahlung verwendet werden können. Weiters könnte der bekannte Datenträger eine Patienten-Applikation abarbeiten, bei deren Abarbeitung Patientendaten von Ärzten und Krankenkassen ausgelesen und verändert werden können. Eine Vielzahl weiterer Applikationen, wie beispielsweise Kreditkarten-Applikationen oder Fahrschein-Applikationen, sind dem Fachmann bekannt.

Wenn mit so einem Datenträger, der die Kreditkarten-Applikation abarbeitet, bei einem Kreditkartenterminal eine Zahlung durchgeführt werden soll, dann wird zur Verifikation der Gültigkeit des Datenträgers eine den Datenträger kennzeichnende Datenträgerkenninformation von dem Kreditkartenterminal an ein sogenanntes Trustcenter elektronisch übermittelt. Das Trustcenter prüft die Gültigkeit der Datenträgerkenninformation und gibt im Fall eines positiven Prüfungsergebnisses eine Gültigkeitsinformation elektronisch an das Kreditkartenterminal ab.

Bei dem bekannten Datenträger werden die Applikationen unmittelbar bei der Herstellung des Datenträgers auf jeden Fall aber vor der Ausgabe an Benutzer des Datenträgers in Speichermitteln des Datenträgers gespeichert beziehungsweise installiert.

Wenn mehrere Applikationen auf einem Datenträger installiert wurden, dann muss sichergestellt sein, dass die Applikationen klar von einander getrennt abgearbeitet werden und unerwünschte gegenseitige Zugriffe auf gegebenenfalls geheime oder sicherheitsrelevante Daten (z.B. Geldbeträge, Patientendaten) verhindert werden. Entsprechende Vorkehrungen sind in EP 0 935 214 A offenbart. Auch bei der Veränderung einer in einem Datenträger abgearbeiteten oder abzuarbeitenden Applikation muss sichergestellt sein, dass andere von dem Datenträger abgearbeitete Applikationen nicht beeinträchtigt werden. Weiters muss sichergestellt sein, dass nur zur Veränderung von Applikationen berechtigte Personen oder Einrichtungen auf die Speichermittel des Datenträgers entsprechenden Zugriff erhalten. Zusätzlich muss die Identität des Datenträgers vor einer Installation der Applikation zweifelsfrei sichergestellt werden, damit die Applikation nicht auf einem anderen, durch Dritte manipulierten Datenträger gespeichert wird.

Die Erfindung hat sich zur Aufgabe gestellt, ein Erteilungsverfahren gemäß der in dem ersten Absatz angegebenen Gattung, einen Datenträger gemäß der in dem zweiten Absatz angegebenen Gattung und eine Veränderungseinrichtung gemäß der in dem dritten Absatz angegebenen Gattung zu schaffen, bei der die vorstehend angegebenen Vorkehrungen getroffen sind. Zur Lösung vorstehend angegebener Aufgabe sind bei einem solchen Erteilungsverfahren folgende Verfahrensschritte vorgesehen:

Erzeugen einer ersten Schlüsselinformation und einer zugehörigen zweiten Schlüsselinformation für einen oder mehrere durch eine Datenträgerkenninformation gekennzeichneten Datenträger;

Erteilen der Veränderungsberechtigung für durch die Datenträgerkenninformation gekennzeichnete Datenträger durch Abgeben der Datenträgerkenninformation und der zugehörigen zweiten Schlüsselinformation an die Veränderungseinrichtung;

Überprüfen der Zugehörigkeit der in dem Datenträger gespeicherten ersten Schlüsselinformation zu der von der Veränderungseinrichtung an den Datenträger abgegebenen zweiten Schlüsselinformation in dem Datenträger und im Fall eines positiven Prüfungsergebnisses;

Zulassen der Veränderung der Applikation in dem Datenträger durch die

Veränderungseinrichtung.

Zur Lösung vorstehend angegebener Aufgabe ist ein solcher Datenträger durch folgende Merkmale gekennzeichnet: Rechnermitteln zum Abarbeiten der zumindest einen Applikation, wobei über die Schnittstellen kommunizierte oder in dem Datenträger gespeicherte Informationen verarbeitet werden, und mit
Speichermitteln zum Speichern einer ersten Schlüsselinformation und einer zugehörigen den Datenträger kennzeichnenden Datenträgerkenninformation und mit
Prüfmitteln zum Prüfen einer Veränderungsberechtigung einer Veränderungseinrichtung zur Veränderung einer Applikation in dem Datenträger über die Schnittstelle, wobei die Prüfmittel zum Prüfen der Zugehörigkeit der in den Speichermitteln gespeicherten ersten Schlüsselinformation zu der von der Veränderungseinrichtung an den Datenträger abgegebenen zweiten Schlüsselinformation ausgebildet sind und mit
Veränderungsmitteln, die nach dem Bestätigen der Veränderungsberechtigung der Veränderungseinrichtung durch die Prüfmittel, zum Ermöglichen der Veränderung der Applikation in dem Datenträger durch die Veränderungseinrichtung ausgebildet sind.

Zur Lösung vorstehend angegebener Aufgabe ist eine solche Veränderungseinrichtung durch folgende Merkmale gekennzeichnet: zumindest eine Schnittstelle zum kontaktlosen und/oder kontaktbehafteten Kommunizieren von Informationen mit einem durch eine Datenträgerkenninformation gekennzeichneten Datenträger und mit
Speichermitteln zum Speichern zumindest einer einen Datenträger kennzeichnenden Datenträgerkenninformation und zugehörigen zweiten Schlüsselinformation und mit
Rechnermitteln zum Verändern von Applikationen in Datenträgern über die Schnittstelle, wobei bei einer Kommunikation mit einem durch eine gespeicherte Datenträgerkenninformation gekennzeichneten Datenträger die Veränderungsberechtigung der Veränderungseinrichtung durch Kommunikation der dieser Datenträgerkenninformation zugehörigen zweiten Schlüsselinformation an den Datenträger abgegeben wird, worauf nach Bestätigung der Veränderungsberechtigung durch den Datenträger die Veränderungseinrichtung zum Verändern der Applikation in dem Datenträger berechtigt und ausgebildet ist.

Durch die erfindungsgemäßen Merkmale ist erreicht, dass für Datenträger, die durch eine Datenträgerkenninformation gekennzeichnet sind, eine jeweils zugehörige erste

und zweite Schlüsselinformation erzeugt werden kann. Die erste Schlüsselinformation und die Datenträgerkenninformation werden in dem Datenträger gespeichert und die zweite Schlüsselinformation und die Datenträgerkenninformation werden an eine Veränderungseinrichtung abgegeben. Hierdurch erhält die Veränderungseinrichtung die Veränderungsberechtigung zum Verändern einer oder mehrerer Applikationen des oder der durch die Datenträgerkenninformation gekennzeichneten Datenträger. Als Veränderung einer Applikation eines Datenträgers wird hierbei die Erst-Installation der Applikation auf dem Datenträger, das Updaten (z.B. neue Version) einer auf dem Datenträger bereits installierten Applikation sowie das Löschen einer Applikation eines Datenträgers verstanden.

Die Veränderungseinrichtung kann somit vorteilhafterweise zu einem Zeitpunkt, wenn die Datenträger bereits an Benutzer ausgegeben wurden, Applikationen der Datenträger verändern, für die sie die Veränderungsberechtigung durch Erhalt der Datenträgerkenninformation und zugehörigen zweiten Schlüsselinformation erworben hat. Der Erwerb der Veränderungsberechtigung kann an die Zahlung einer Veränderungsberechtigungsgebühr gebunden sein, womit eine interessante Geschäftsmethode erhalten ist. Besonders vorteilhaft ist hierbei, dass die Veränderung einer Applikation eines Datenträgers im Zuge einer Kommunikation des Datenträgers mit der Veränderungseinrichtung erfolgen kann, ohne dass dafür ein Trustcenter zur Bestätigung der Veränderungsberechtigung kontaktiert werden muss.

Gemäß den Maßnahmen der Ansprüche 2 und 11 ist der Vorteil erhalten, dass die Veränderungsberechtigung die Veränderungseinrichtung beispielsweise nur zur Installation einer neuen Applikation, nicht jedoch zum Updaten oder Löschen der Applikation berechtigen kann. Ebenso könnte die Veränderungsberechtigung die Veränderungseinrichtung auch nur zum Löschen einer Applikation und gegebenenfalls auch gleich zur Installation einer neuen Applikation in dem durch das Löschen frei gewordenen Speicherbereich der Speichermittel in dem Datenträger berechtigen. Wenn eine neue Version einer Applikation auf allen bereits an Benutzer ausgegebenen Datenträgern anstatt der alten Version der Applikation installiert werden soll, dann könnte eine entsprechende Veränderungsberechtigung von dem Betreiber der Applikation (z.B. Bank-Applikation) an den Betreiber von Veränderungseinrichtungen (z.B. Bankautomaten) abgegeben werden. Eine Vielzahl solcher vorteilhafter Anwendungsfälle sind ermöglicht,

wobei der Erwerb der Veränderungsberechtigung jeweils an Gegenleistungen gebunden sein kann, womit eine interessante Geschäftsmethode erhalten ist.

Gemäß den Maßnahmen der Ansprüche 3 und 12 ist der Vorteil erhalten, dass durch die Veränderungsberechtigung, also durch die Datenträgerkenninformation und zugehörige zweite Schlüsselinformation, die Applikation gekennzeichnet ist, die verändert werden darf. Für einen Datenträger der zwei Applikationen abarbeitet, können daher vorteilhafterweise für jede der beiden Applikationen die vorstehend beschriebenen unterschiedlichen Veränderungsberechtigungen (installieren, updaten, löschen) vergeben werden.

Gemäß den Maßnahmen der Ansprüche 4 und 13 ist der Vorteil erhalten, dass eine Veränderungsberechtigung zur Installation einer neuen Applikation in dem Datenträger vergeben werden kann, wobei die neue Applikation nicht mehr als einen maximalen Speicherplatzbedarf (z.B. 1 kBit) in den Speichermitteln beanspruchen darf. Hierdurch ist ein besonders interessantes Geschäftsmodell erhalten, bei dem Speicherplatz in bereits an Benutzer vergebenen Datenträgern verkauft werden kann. So könnte ein Kreditkartenhersteller in den Speichermitteln seiner Kreditkarte Speicherplatz für zukünftige Applikationen reservieren und zu einem Zeitpunkt, wenn bereits eine große Anzahl an Kreditkarten an Benutzer ausgegeben wurden, diesen Speicherplatz in Form von entsprechenden Veränderungsberechtigungen an ein oder mehrere Firmen verkaufen, um auch deren Applikationen (z.B. Kundenkarte, elektronischer Fahrschein) mit der Kreditkarte abzuarbeiten.

Gemäß den Maßnahmen des Anspruchs 5 ist der Vorteil erhalten, mit nur einer Veränderungsberechtigung, die durch nur eine Datenträgerkenninformation und nur eine zweite Schlüsselinformation gebildet ist, eine Applikation in einer Gruppe von Datenträgern verändert werden kann, wobei die Datenträger alle durch die gleiche Datenträgerkenninformation gekennzeichnet sind.

Gemäß den Maßnahmen der Ansprüche 6 und 14 ist der Vorteil erhalten, dass eine Veränderungsberechtigung bestimmte Zugriffsrechte der Applikation kennzeichnet, die verändert werden darf. Beispielsweise könnte eine Veränderungsberechtigung für eine Kreditkarte vergeben werden, die zur Installation einer Applikation berechtigt, die nur die kontaktbehaftete und nicht die kontaktlose Schnittstelle nutzen darf und ausschließlich Leserechte in bestimmten für alle Applikationen der Kreditkarte gemeinsamen

Speicherbereichen erlaubt.

Gemäß den Maßnahmen des Anspruchs 7 ist der Vorteil erhalten, dass die Veränderungseinrichtung mit einer der in dem Datenträger gespeicherten ersten Master Keyinformation zugehörigen zweiten Master Keyinformation Zugriffsrechte für einzelne oder alle von dem Datenträger abgearbeiteten Applikationen auf Schnittstellen oder Speicherbereiche ändern kann. Ebenso könnte mit Hilfe der Master Keyinformationen eine neue erste Schlüsselinformation in dem Datenträger und eine neue zweite Schlüsselinformation in der Veränderungseinrichtung erzeugt und gespeichert werden, um eine weitere Applikation verändern zu können.

Gemäß den Maßnahmen des Anspruchs 8 ist der Vorteil erhalten, dass mit Hilfe der Master Keyinformationen das Verändern der Zugriffsrechte und/oder das Erzeugen von Schlüsselinformationen auf nur eine bestimmte Applikation eingeschränkt werden kann.

Gemäß den Maßnahmen des Anspruchs 9 ist der Vorteil erhalten, dass zusätzlich zur Überprüfung der Schlüsselinformation von dem Datenträger bestimmte Eigenschaften der zu verändernden Applikation geprüft werden, bevor eine Veränderung der Applikation ermöglicht wird. Hierbei könnte beispielsweise der Betreiber der Applikation eine dritte Schlüsselinformation in der Applikation speichern, deren Richtigkeit vor der Veränderung der Applikation durch den Datenträger geprüft wird.

Gemäß den Maßnahmen des Anspruchs 15 ist der Vorteil erhalten, dass sogenannte Java Applets von Datenträgern besonders vorteilhaft abarbeitbar sind.

Gemäß den Maßnahmen des Anspruchs 16 ist der Vorteil erhalten, dass die Veränderungseinrichtung durch einen Betreibercomputer des Betreibers einer Applikation und eine Leseeinrichtung (z.B. Bankautomat) gebildet sein können, die über ein Datennetz (z.B. Internet, Firmennetz, Telephonnetz,...) miteinander verbunden sind. Auf diese Weise sind eine Vielzahl vorteilhafter Anwendungen ermöglicht.

Die Erfindung wird im Folgenden anhand von einem in den Figuren dargestellten Ausführungsbeispiel beschrieben, auf das die Erfindung aber nicht beschränkt ist.

Die Figur 1 zeigt einen Datenträger, in dem eine Veränderungseinrichtung eine

weitere Applikation installiert.

Die Figur 2 zeigt ein Veränderungsverfahren zum Verändern einer Applikation in dem Datenträger gemäß Figur 1.

Die Figur 1 zeigt symbolische den Herstellungsprozess H einer Smart Card S, die einen Datenträger bildet und die nach abgeschlossenem Herstellungsprozess H zum kontaktlosen Kommunizieren mit einem Terminal 1 und zum kontaktbehafteten Kommunizieren mit einem Lesegerät 2 ausgebildet ist. Bei dem Herstellungsprozess H wird ein integrierter Schaltkreis in eine Plastikkarte eingebracht und mit einer Antenne 3, zum kontaktlosen Kommunizieren, und mit einem Kontaktfeld 4, zum kontaktbehafteten Kommunizieren, verbunden. Ein solcher Herstellungsprozess H ist seit langem bekannt, weshalb hierauf nicht näher eingegangen ist.

Figur 2 zeigt ein Erteilungsverfahren E, um einer Veränderungseinrichtung 5 eine Veränderungsberechtigung zum Verändern einer Applikation in der Smart Card S zu erteilen. Als Applikation wird hierbei die Art der Verwendung (z.B: als Kreditkarte, als Museumsticket,...) der Smart Card S und werden somit Rechnermitteln 6 der Smart Card S verstanden, die ein Softwareprogramm zur Ermöglichung dieser Verwendung abarbeiten.

Bei dem Herstellungsprozess H der Smart Card S werden ein oder mehrere Applikationen, beziehungsweise die entsprechenden Softwareprogramme, in Speichermitteln 7 der Smart Card S gespeichert. Weiters erhält jede Smart Card S bei dem Herstellungsprozess H eine Datenträgerkenninformation also gemäß diesem Ausführungsbeispiel eine fortlaufende Seriennummer ID, die in Sicherheitsspeichermitteln 8 der Smart Card S gespeichert wird und mit der jede Smart Card S eindeutig identifizierbar ist. Die Seriennummer ID ist hierbei durch eine 64 Stellen aufweisende binäre Bitkombination gebildet und die Sicherheitsspeichermittel 8 sind durch einen gegen Angriffe eines Hackers besonders geschützten Bereich der Speichermittel 7 gebildet.

Gemäß Block B1 des Erteilungsverfahrens E erzeugt ein Computer C bei dem Herstellungsprozess H eine erste Schlüsselinformation K1 und eine zugehörige zweite Schlüsselinformation K2 für jede durch ihre Seriennummer ID gekennzeichnete Smart Card S. Weiters wird für einige oder alle durch eine Seriennummer ID gekennzeichnete Smart Cards S eine erste Master Keyinformation MKI1 und eine zweite Master

Keyinformation MKI2 erzeugt, worauf nachfolgend näher eingegangen ist. Die Schlüsselinformationen K1 und K2 sowie die Master Keyinformationen MKI1 und MKI2 können hierbei durch sogenannte symmetrische binäre Schlüssel oder durch sogenannte unsymmetrische binäre Schlüssel gebildet sein, wie dies dem Fachmann seit langen bekannt ist. Dem Fachmann sind auch andere jeweils zwei Schlüsselinformationen aufweisende Verschlüsselungsverfahren bekannt, die in diesem Zusammenhang ebenfalls verwendbar sind.

Die von dem Computer C erzeugte erste Schlüsselinformation K1 und gegebenenfalls erzeugte erste Master Keyinformation MKI1 werden der Seriennummer ID der Smart Card S zugeordnet in den Sicherheitsspeichermitteln 8 der Smart Card S gespeichert und von einer von der Smart Card S abgearbeiteten Sicherheitsapplikation AS verarbeitet, wie dies nachfolgend näher beschrieben ist. Gegebenenfalls alle von dem Computer C erzeugten Informationen, auf jeden Fall aber die Seriennummer ID, die zweite Schlüsselinformation K2 und die gegebenenfalls zusätzlich erzeugte zweite Master Keyinformation MKI2 werden in Sicherheitsspeichermitteln 9 des Herstellers der Smart Cards S gespeichert. Die in den Sicherheitsspeichermitteln 9 gespeicherten Informationen können nunmehr in weiterer Folge zum Erteilen von Veränderungsberechtigungen zum Verändern von Applikationen in der Smart Card S verwendet werden, worauf anhand von Anwendungsbeispielen nachfolgend eingegangen ist.

Gemäß einem ersten Anwendungsbeispiel ist angenommen, dass der Hersteller der Smart Cards S eine Million Stück Smart Cards S für ein Kreditkartenunternehmen herstellt. Hierfür wird bei der Herstellung der Smart Cards S eine Kreditkartensoftware in den Speichermitteln 7 gespeichert und von den Rechenmitteln 6 als erste Applikation A1 abgearbeitet. In den Sicherheitsspeichermitteln 8 der Smart Card S wird bei der Herstellung die Seriennummer ID = „123...84“, die erste Schlüsselinformation K1 = „2..4“ und die erste Master Keyinformation MKI1 = „88...3“ gespeichert. In den Sicherheitsspeichermitteln 9 des Herstellers wird der Seriennummer ID = „123....84“, die der ersten Schlüsselinformation K1 zugehörige zweite Schlüsselinformation K2 = „3....5“ und die der ersten Master Keyinformation MKI1 zugehörige zweite Master Keyinformation MKI2 = „99....4“ zugeordnet gespeichert. Mit einer Wirkverbindung W ist angedeutet, dass sämtliche erzeugte Smart Cards S an Kunden des Kreditkartenunternehmens ausgegeben werden. In weiterer Folge werden die Smart Cards S zur Bezahlung von Rechnungen in

Geschäften verwendet, wie dies allgemein bekannt ist.

Bei der Herstellung der Smart Cards S wurde darauf geachtet, dass die Speichermittel 7 auch nach dem Einspeichern der Kreditkartensoftware noch ausreichend zusätzlichen Speicherplatz aufweisen. Beispielsweise könnte die Kreditkartensoftware 3 kBit des Speicherplatzes der Speichermittel 7 und die Sicherheitsspeichermittel 8 4 kBit belegen, wobei noch 17 kBit der insgesamt 24 kBit der durch ein EEPROM gebildeten Speichermittel 7 frei bleiben. Weiters wurden die Rechnermittel 6 bezüglich ihrer Rechnerleistung so bemessen, dass bis zu vier Applikationen A1, A2, A3 und A4 parallel oder auch zeitversetzt abgearbeitet werden können.

Gemäß dem Anwendungsbeispiel ist nun angenommen, dass eine große Warenhauskette Kundenkarten an ihre Kunden ausgeben möchte, um diesen Kunden besondere Einkaufskonditionen oder Rückvergütungen zu gewähren. Da sehr vielen Kunden der Warenhauskette ihre Einkäufe mit den Smart Cards S des Kreditkartenunternehmens bezahlten und es für die Kunden angenehmer ist, nicht noch eine weitere Plastikkarte als Kundenkarte mitnehmen zu müssen, erwirbt die Warenhauskette bei dem Kreditkartenunternehmen eine Veränderungsberechtigung zur Installation ihrer Kundenkartesoftware als zweite Applikation A2 auf den Smart Cards S.

Bei einem Block B2 des Erteilungsverfahrens E fragt die Warenhauskette als zukünftiger Betreiber der Applikation A2 bei dem Kreditkartenunternehmen beziehungsweise bei dem Hersteller der Smart Cards S um eine Veränderungsberechtigung an und bezahlt den hierfür geforderten Kaufpreis. Hierbei kauft die Warenhauskette im wesentlichen den Speicherplatz in den Speichermitteln 7 sämtlicher an Kunden bereits ausgegebener Smart Cards S, um die Kundenkartensoftware in den Speichermitteln 7 zu speichern. Der Kaufpreis wird hierbei von dem Speicherplatzbedarf und der Anzahl der an Kunden ausgegebenen Smart Cards S abhängig sein. Weiters kann der Kaufpreis davon abhängig gemacht werden, welche Schnittstellen - nur die kontaktlose oder nur die kontaktbehaftete oder beide Schnittstellen – von der zweiten Applikation A2 benötigt werden, sowie welche Rechnerleistung für die Abarbeitung der zweiten Applikation A2 nötig sein wird. Zusätzlich wird der Kaufpreis davon abhängig sein, ob auch Master Keyinformationen für die Smart Cards S erzeugt wurden und ob die zweiten Master Keyinformationen MKI2 mit verkauft werden. Durch den Verkauf von Veränderungsberechtigungen ist somit ein interessantes Geschäftsmodell erhalten.

Nach einer Einigung des Kreditkartenunternehmens beziehungsweise des Herstellers der Smart Cards S mit dem Betreiber der zweiten Applikation A2, der Warenhauskette, werden bei einem Block B3 die Veränderungsberechtigungen, also die Seriennummern ID samt zugehörigen zweiten Schlüsselinformationen K2 je Smart Card S und gegebenenfalls auch zweite Master Keyinformationen MKI2, an einen Betreibercomputer 10 des Betreibers der zweiten Applikation A2 übermittelt. Dieses Übermitteln kann – wie in Figur 1 dargestellt – über ein Datennetz NET erfolgen, wobei allerdings höchste Sicherheitsvorkehrungen, beispielsweise durch das Einschalten eines Trustcenters, getroffen werden müssen, um zu verhindern, dass die Veränderungsberechtigungen von nicht berechtigte Personen empfangen werden. Die Veränderungsberechtigungen könnten allerdings auch durch manuelle Übergabe einer die entsprechenden Informationen speichernde CD-ROM, Harddisk oder DVD an den Betreiber der Applikation A2 erfolgen. Die Veränderungsberechtigungen stehen hierauf in dem Betreibercomputer 10 zur Verfügung.

Gemäß dem Anwendungsbeispiel ist angenommen, dass zur Installation der zweiten Applikation aus Sicherheitsgründen ausschließlich die kontaktbehaftete Schnittstelle der Smart Cards S verwendet werden soll. Hierfür wird die Veränderungseinrichtung 5 zum Installieren der zweiten Applikation durch den Betreibercomputer 10 und eine Vielzahl an über ein Datennetz NET mit dem Betreibercomputer 10 verbundene Lesegeräte 2 gebildet. Sobald ein Kunde seine Ware mit der Kreditkartenapplikation der Smart Card S bezahlen möchte und der Verkäufer die Smart Card S in das Lesegerät 2 einführt beginnt bei einem Block B4 der Installationsvorgang der zweiten Applikation auf der Smart Card S.

Am Anfang des Installationsvorgangs übermittelt die Smart Card S über Schnittstellenmittel 11, das Kontaktfeld 4 und ein Kontaktfeld 12 des Lesegeräts 2 ihre Seriennummer ID. Eine Rechnerstufe 13 des Lesegeräts 2 übermittelt die Seriennummer ID an den Betreibercomputer 10, der hierauf prüft, ob es sich bei der Smart Card S um eine gültige Smart Card S handelt. Gegebenenfalls könnte die Smart Card S mit ihrer ersten Schlüsselinformation K1 ein Codewort verschlüsseln und über das Lesegerät 2 an den Betreibercomputer 10 übermitteln, welches verschlüsselte Codewort in dem Betreibercomputer 10 nur durch die zugehörige zweite Schlüsselinformation K2 entschlüsselt werden kann. Dieses Prüfen der Gültigkeit der Smart Card S dient um zu

verhindern, dass die zweite Applikation A2 auf einer ungültigen Smart Card S installiert wird.

Wenn bei dem Block B4 die Gültigkeit der Smart Card S festgestellt wurde, dann wird die Installation der zweiten Applikation A2 bei einem Block B5 fortgesetzt und andernfalls beendet. Bei dem Block B5 wird die der Seriennummer ID der Smart Card S in dem Betreibercomputer 10 zugeordnete zweite Schlüsselinformation K2 ermittelt und über das Lesegerät 2 an die Sicherheitsapplikation AS der Smart Card S abgegeben. Gegebenenfalls kann aus Sicherheitsgründen auch eine Verschlüsselung der zweiten Schlüsselinformation K2 durchgeführt werden. Die Sicherheitsapplikation AS prüft hierauf bei einem Block B6, ob die in den Sicherheitsspeichermitteln 8 gespeicherte erste Schlüsselinformation K1 zu der von der Veränderungseinrichtung 5 abgegebenen zweiten Schlüsselinformation K2 zugehörig ist, wobei festgestellt wird, ob die Veränderungseinrichtung 5 eine Veränderungsberechtigung zur Veränderung beziehungsweise zur Installation der zweiten Applikation A2 hat.

Wenn die Prüfung bei dem Block B6 ergibt, dass die Veränderungseinrichtung 5 zur Installation der zweiten Applikation A2 berechtigt ist, dann wird die zweite Applikation A2 in einem Block B7 in den Speichermitteln 7 der Smart Card S gespeichert. Hierfür übermittelt der Betriebscomputer 10 die zweite Applikation A2 über die Leseeinrichtung 2 und die Smart Card S lässt den Zugriff der Leseeinrichtung 2 auf die Speichermittel 7 in bestimmtem Umfang zu. Der Umfang beziehungsweise die Art der Veränderung der zweiten Applikation A2 durch die Veränderungseinrichtung 5 wird hierbei durch die Art der Veränderungsberechtigung, also durch die zweite Schlüsselinformation K2 festgelegt und durch die Sicherheitsapplikation AS in der Smart Cards S festgestellt.

Die Veränderungsberechtigung kann den Betreiber der zweiten Applikation A2 zur Installation der zweiten Applikation A2 in einem bezüglich seines Speicherplatzes begrenzten (z.B. maximal 5 kBit) Teil in den Speichermitteln 7 berechtigen. Hierdurch ist sichergestellt, dass tatsächlich für vier Applikationen A1 bis A4 ausreichend Speicherplatz in den Speichermitteln 7 vorhanden ist.

Weiters können durch die Veränderungsberechtigung die Zugriffsrechte der zweiten Applikation A2 auf für die Applikationen gemeinsame Speicherbereiche der Speichermittel 7 und auf die Schnittstellen des Smart Card S festgelegt sein. Hierbei

könnte die Kundenkartenapplikation beispielsweise ausschließlich die kontaktlose Schnittstelle zur Kommunikation von Kundendaten und Rückvergütungen verwenden.

Weiters kann durch die Veränderungsberechtigung festgelegt sein, zu welcher Art der Veränderung einer Applikation die Veränderungseinrichtung 5 berechtigt ist. Hierbei könnte die Veränderungseinrichtung 5 auch nur zum Ersetzten der zweiten Applikation A2 durch eine neuere Version der Kundenkartenapplikation oder durch eine gänzlich andere zweite Applikation A2 berechtigt sein. Ebenso könnte die Veränderungsberechtigung ausschließlich das Löschen der zweiten Applikation ermöglichen. Ebenso können Kombinationen dieser Möglichkeiten oder alle diese Möglichkeiten mit nur einer zweiten Schlüsselinformation K2 möglich sein.

Weiters kann beziehungsweise muss die Veränderungsberechtigung auch die Applikation kennzeichnen, die verändert werden darf, um zu verhindern, dass beispielsweise eine falsche Applikation aus den Speichermitteln 7 der Smart Card S gelöscht wird. Die Veränderungsberechtigung könnte aber auch nur einen bestimmten Speicherbereich in den Speichermitten 7 kennzeichnen in dem eine beliebige oder eine vorgeschriebene Änderung durchgeführt werden darf.

Wenn in der Smart Card S die erste Master Keyinformation MKI1 gespeichert wurde und wenn an die Veränderungseinrichtung 5 die zugehörige zweite Master Keyinformation MKI2 für die Smart Card S abgegeben wurde, dann ist der Veränderungseinrichtung 5 das Verändern von Zugriffsrechten in der Smart Card S und/oder das Erzeugen weiterer erster Schlüsselinformationen K1 in der Smart Card S und weiterer zweiter Schlüsselinformationen K2 in dem Betreibercomputer 10 ermöglicht. Es sei angenommen, dass die Warenhauskette nicht mehr ausschließlich kontaktlos kommunizierende Terminals 1 zur Kommunikation von Kundendaten, sondern zusätzlich auch die kontaktbehaftet kommunizierenden Leseeinrichtungen 2 einsetzen möchte. Da die zweite Applikation A2 bei ihrer Installation nur die Zugriffsrechte auf die kontaktlose Schnittstelle (Schnittstelle 11 und Antenne 3) erhalten hat, ist dies aber nicht möglich. Die Veränderungseinrichtung 5 kann nunmehr durch Verschlüsselung eines Zugriffsrecht-Veränderungsbefehls mit der zweiten Master Keyinformation MKI2 und Übermittlung des verschlüsselten Codes an die Smart Card S erreichen, dass die Sicherheitsapplikation AS durch Entschlüsselung des empfangenen Codes mit der in den Sicherheitsspeichermitteln 8 gespeicherten ersten Master Keyinformation MKI1 die Veränderungsberechtigung der

Veränderungseinrichtung 10 feststellt und den Zugriffsrecht-Veränderungsbefehl ausführt. Hierdurch erhält die zweite Applikation A2 sowohl auf die kontaktlose Schnittstelle als auch auf die kontaktbehaftete Schnittstelle der Smart Card S Zugriff. Somit können vorteilhafterweise auch bei Applikationen, die von an Kunden bereits ausgegebenen Smart Cards S abgearbeitet werden, die Zugriffsrechte auf Schnittstellen und ebenso auf Speicherbereiche der Speichermittel 7 verändert werden.

Weiters könnte der Fall eintreten, dass die in den Sicherheitsspeichermitteln 8 gespeicherte erste Schlüsselinformation K1 bereits zur Veränderung einer Applikation verwendet wurde oder von Hackern ausspioniert wurde und somit gegebenenfalls nicht mehr verwendbar ist. In diesem Fall könnte mit dem Betreibercomputer 10 eine neue erste und zweite Schlüsselinformation erzeugt werden, wobei die neue erste Schlüsselinformation mit der ersten Master Keyinformation MKI1 verschlüsselt als Code an die Smart Card S übermittelt werden könnte. Die Sicherheitsapplikation AS der Smart Card S könnte hierauf den empfangenen Code mit der zweiten Master Keyinformation MKI2 entschlüsseln, worauf vorteilhafterweise die neue erste Schlüsselinformation in den Sicherheitsspeichermitteln 8 der Smart Card S zur Veränderung einer weiteren Applikation gespeichert werden könnte.

Die erste Master Keyinformation MKI1 und die zweite Maser Keyinformation MKI2 könnten auch derart erzeugt werden, dass nicht die gesamte Smart Card S betreffende Veränderungen durchgeführt werden könnten, sonder nur auf eine Applikation bezogene Veränderungen der Zugriffsrechte oder die Erzeugung neuer Schlüsselinformationen für nur diese eine Applikation durchgeführt werden könnten. Hierdurch könnte sichergestellt werden, dass bestimmte kritische Applikationen (z.B. Kreditkartenapplikation, Bankapplikation,...) keinesfalls, also auch nicht mit Hilfe einer Master Keyinformation, verändert werden könnten, da die Berechtigung der Master Keyinformationen auf andere Applikationen eingeschränkt wäre.

Als weitere Sicherheitsvorkehrung könnte festgelegt sein, dass die Veränderung der Applikation in der Smart Card S durch die Veränderungseinrichtung 5 von der Smart Card S nur dann zugelassen wird, wenn bestimmte Eigenschaften der zu verändernden Applikation festgestellt werden. Beispielsweise könnte von dem Betreiber der Applikation in die Applikation eine dem Hersteller der Smart Card gegebenenfalls nicht bekannte weitere Schlüsselinformation eingebracht worden sein, deren versteckte

weitere Schlüsselinformation eine Eigenschaft der Applikation bildet. Die Smart Cards S würde eine Veränderung (z.B. löschen) dieser in der Smart Card S gespeicherten Applikation durch die Veränderungseinrichtung 5 nur dann zugelassen, wenn die Veränderungseinrichtung 5 eine der weiteren Schlüsselinformation zugehörige Schlüsselinformation an die Smart Card S übermittelt. Hierdurch ist der Vorteil erhalten, dass der Betreiber der Applikation weitere Sicherheitsvorkehrungen für seine Applikation treffen kann.

Gemäß einem zweiten in den Figuren nicht dargestellten Ausführungsbeispiel könnte der Benutzer der Smart Cards S einen Computer samt einem angeschlossenen kontaktlos kommunizierendem Terminal besitzen, der hierbei eine Veränderungseinrichtung bildet. Gemäß dem zweiten Ausführungsbeispiel ist der Computer über das Internet mit einem Server eines Nachrichtensenders verbunden, von dem Nachrichten abrufbar sind und von dem ein Nachrichten-Abonnement angeboten wird. Der Benutzer füllt ein Anmeldeformular für das Nachrichten-Abonnement elektronisch aus und gibt seine Kreditkartennummer zur Bezahlung des Nachrichten-Abonnements an (Block B2). Anschließend wird über das Internet auf den Computer des Benutzers eine Veränderungsberechtigung (ID und K1) gespeichert, mit der eine Nachrichten-Applikation in die Smart Card installiert werden kann. Gemäß dem vorstehend beschriebenen Installationsvorgang wird hierauf die Nachrichten-Applikation als dritte Applikation in der Smart Card gespeichert. Der Benutzer hat anschließend mit der Smart Card die Möglichkeit bei beliebigen Computern mit kontaktlos kommunizierenden Terminals besonders aktuelle Nachrichten des Nachrichten-Abonnements abzurufen. Weiters war in dem Nachrichten-Abonnement auch eine Kinokarte für einen Kinobesuch enthalten. Der Benutzer kann somit bei einem Terminal einer Kinokasse seine Smart Card vorweisen, worauf die Nachrichten-Applikation der Smart Card bei einer kontaktlosen Kommunikation einmalig eine Kinokarte bestätigt. Dieses Service ist möglich, da der Betreiber des Kinos mit dem Betreiber des Nachrichtensenders kooperiert.

Als Datenträger könnte auch ein Transponder ein Personal Digital Assistant ein Mobiltelephon oder anderes ähnliches Gerät verwendet werden. Die kontaktlose Kommunikation kann beispielsweise gemäß einem der veröffentlichten Standards ISO14.443, ISO15.693, ISO18.000, ECMA 340 oder auch gemäß einem der Telephonstandards GSM oder UMTS, erfolgen.

Durch das erfindungsgemäße Erteilungsverfahren, den erfindungsgemäßen Datenträger und die erfindungsgemäße Veränderungseinrichtung ist somit zusätzlich zu den vorstehend beschriebenen Vorteilen der wesentliche Vorteil erhalten, dass in bereits an Kunden ausgegebenen Datenträgern Applikationen verändert und somit zusätzliche Services mit den Datenträgern ermöglicht werden können, ohne dass dafür ein Trustcenter eingebunden werden muss. Durch das Vermeiden eines Trustcenters kann die Veränderung von Applikationen auch durch „off-line" arbeitende Veränderungseinrichtungen durchgeführt werden und es können Kosten für das Trustcenter eingespart werden. Durch den Verkauf der Veränderungsberechtigungen ist eine interessante Geschäftsmethode erhalten.

Patentansprüche:

1. Erteilungsverfahren (E), um einer Veränderungseinrichtung (5) eine Veränderungsberechtigung zum Verändern einer Applikation in einem Datenträger (S) zu erteilen, wobei folgende Schritte abgearbeitet werden:

Erzeugen einer ersten Schlüsselinformation (K1) und einer zugehörigen zweiten Schlüsselinformation (K2) für einen oder mehrere durch eine Datenträgerkenninformation (ID) gekennzeichneten Datenträger (S);

Erteilen der Veränderungsberechtigung für durch die Datenträgerkenninformation (ID) gekennzeichnete Datenträger (S) durch Abgeben der Datenträgerkenninformation (ID) und der zugehörigen zweiten Schlüsselinformation (K2) an die Veränderungseinrichtung (5);

Überprüfen der Zugehörigkeit der in dem Datenträger (S) gespeicherten ersten Schlüsselinformation (K1) zu der von der Veränderungseinrichtung (5) an den Datenträger (S) abgegebenen zweiten Schlüsselinformation (K2) in dem Datenträger (S) und im Fall eines positiven Prüfungsergebnisses;

Zulassen der Veränderung der Applikation (A1, A2, A3, A4) in dem Datenträger (S) durch die Veränderungseinrichtung (5).

2. Erteilungsverfahren (E) gemäß Anspruch 1, wobei die Veränderungsberechtigung zum Installieren und/oder zum Updaten und/oder zum Löschen der Applikation (A1, A2, A3, A4) in dem Datenträger (S) berechtigt.

3. Erteilungsverfahren (E) gemäß Anspruch 1, wobei die Veränderungsberechtigung nur zur Veränderung einer bestimmten Applikation (A1, A2, A3, A4) in dem Datenträger (S) berechtigt.

4. Erteilungsverfahren (E) gemäß Anspruch 1, wobei die Veränderungsberechtigung nur zur Installation einer Applikation (A1, A2, A3, A4) mit einem vorgegebenen maximalen Speicherplatzbedarf in dem Datenträger (S) berechtigt.

5. Erteilungsverfahren (E) gemäß Anspruch 1, wobei die Datenträgerkenninformation (ID) eine Gruppe von Datenträgern (S) kennzeichnet.

6. Erteilungsverfahren (E) gemäß Anspruch 1, wobei die Veränderungsberechtigung auch die Zugriffsrechte der in dem Datenträger (S) zu verändernden Applikation (A1, A2, A3, A4) auf Speicherbereiche und Schnittstellen (3, 4, 111) des Datenträgers (S) festlegt.

7. Erteilungsverfahren (E) gemäß Anspruch 1, wobei folgende weitere Schritte

abgearbeitet werden:

Erzeugen einer ersten Master Keyinformation (MKI1) und einer zugehörigen zweiten Master Keyinformation (MKI2) für einen oder mehrere durch eine Datenträgerkenninformation (ID) gekennzeichnete Datenträger (S), wobei nur mit der in dem Datenträger (S) gespeicherten ersten Master Keyinformation (MKI1) und nur mit der in der Veränderungseinrichtung (5) gespeicherten zweiten Master Keyinformation (MKI2) das Verändern von Zugriffsrechten in dem Datenträger (S) und/oder das Erzeugen weiterer Schlüsselinformationen in dem Datenträger (S) und der Veränderungseinrichtung (5) möglich ist.

8. Erteilungsverfahren (E) gemäß Anspruch 7, wobei die erste Master Keyinformation (MKI1) und die zugehörige zweite Master Keyinformation (MKI2) nur das Verändern von Zugriffsrechten einer bestimmten Applikation (A1, A2, A3, A4) in dem Datenträger (S) und/oder das Erzeugen weiterer Schlüsselinformationen in dem Datenträger (S) und der Veränderungseinrichtung (5) zur Veränderung einer bestimmten Applikation (A1, A2, A3, A4) ermöglicht.

9. Erteilungsverfahren (E) gemäß Anspruch 1, wobei die Veränderung der Applikation (A1, A2, A3, A4) in dem Datenträger (S) durch die Veränderungseinrichtung (5) von dem Datenträger (S) nur dann zugelassen wird, wenn bestimmte Eigenschaften der zu verändernden Applikation (A1, A2, A3, A4) festgestellt werden.

10. Datenträger (S) zum Abarbeiten zumindest einer Applikation (A1, A2, A3, A4) mit

zumindest einer Schnittstelle (3, 4, 11) zum kontaktlosen und/oder kontaktbehafteten Kommunizieren von Informationen und mit

Rechnermitteln (6) zum Abarbeiten der zumindest einen Applikation (A1, A2, A3, A4), wobei über die Schnittstellen (3, 4, 11) kommunizierte oder in dem Datenträger (S) gespeicherte Informationen verarbeitet werden, und mit

Speichermitteln (8) zum Speichern einer ersten Schlüsselinformation und einer zugehörigen den Datenträger (S) kennzeichnenden Datenträgerkenninformation (ID) und mit

Prüfmitteln (6, AS) zum Prüfen einer Veränderungsberechtigung einer Veränderungseinrichtung (5) zur Veränderung einer Applikation (A1, A2, A3, A4) in dem Datenträger (S) über die Schnittstelle (3, 4, 11), wobei die Prüfmittel (6, AS) zum Prüfen

der Zugehörigkeit der in den Speichermitteln (8) gespeicherten ersten Schlüsselinformation (K1) zu der von der Veränderungseinrichtung (5) an den Datenträger (S) abgegebenen zweiten Schlüsselinformation (K2) ausgebildet sind und mit

Veränderungsmitteln (6), die nach dem Bestätigen der Veränderungsberechtigung der Veränderungseinrichtung (5) durch die Prüfmittel (6, AS), zum Ermöglichen der Veränderung der Applikation (A1, A2, A3, A4) in dem Datenträger (S) durch die Veränderungseinrichtung (5) ausgebildet sind.

11. Datenträger (S) gemäß Anspruch 10, wobei die Prüfmittel (6, AS) zum Bestätigen einer beschränkten Veränderungsberechtigung ausgebildet sind, die nur zum Installieren und/oder zum Updaten und/oder zum Löschen der Applikation (A1, A2, A3, A4) in dem Datenträger (S) berechtigt.

12. Datenträger (S) gemäß Anspruch 10, wobei die Prüfmittel (6, AS) zum Bestätigen einer beschränkten Veränderungsberechtigung ausgebildet sind, die nur zur Veränderung einer bestimmten Applikation (A1, A2, A3, A4) in dem Datenträger (S) berechtigt.

13. Datenträger (S) gemäß Anspruch 10, wobei die Prüfmittel (6, AS) zum Bestätigen einer beschränkten Veränderungsberechtigung ausgebildet sind, die nur zur Installation einer Applikation (A1, A2, A3, A4) mit einem vorgegebenen maximalen Speicherplatzbedarf in dem Datenträger (S) berechtigt.

14. Datenträger (S) gemäß Anspruch 10, wobei die Prüfmittel (6, AS) zum Bestätigen einer Veränderungsberechtigung ausgebildet sind, die die Zugriffsrechte der in dem Datenträger (S) zu verändernden Applikation (A1, A2, A3, A4) auf Speicherbereiche der Speichermittel (7) und Schnittstellen (3, 4, 11) des Datenträgers (S) festlegt.

15. Datenträger (S) gemäß Anspruch 10, wobei die Rechenmittel (6) zum Abarbeiten einer durch ein Java Applet gebildeten Applikation (A1, A2, A3, A4) ausgebildet sind.

16. Veränderungseinrichtung (5) zum Verändern einer Applikation (A1, A2, A3, A4) in einem Datenträger (S) mit

zumindest einer Schnittstelle (12) zum kontaktlosen und/oder kontaktbehafteten Kommunizieren von Informationen mit einem durch eine Datenträgerkenninformation (ID) gekennzeichneten Datenträger (S) und mit

Speichermitteln zum Speichern zumindest einer einen Datenträger (S) kennzeichnenden

Datenträgerkenninformation (ID) und zugehörigen zweiten Schlüsselinformation (K2) und mit

Rechnermitteln (13) zum Verändern von Applikationen (A1, A2, A3, A4) in Datenträgern (S) über die Schnittstelle (12), wobei bei einer Kommunikation mit einem durch eine gespeicherte Datenträgerkenninformation (ID) gekennzeichneten Datenträger (S) die Veränderungsberechtigung der Veränderungseinrichtung (5) durch Kommunikation der dieser Datenträgerkenninformation (ID) zugehörigen zweiten Schlüsselinformation (K2) an den Datenträger (S) abgegeben wird, worauf nach Bestätigung der Veränderungsberechtigung durch den Datenträger (S) die Veränderungseinrichtung (5) zum Verändern der Applikation (A1, A2, A3, A4) in dem Datenträger (S) berechtigt und ausgebildet ist.

17. Veränderungseinrichtung (5) gemäß Anspruch 16, wobei die Veränderungseinrichtung (5) durch einen die Speichermittel enthaltenden Betreibercomputer (10) und durch eine mit dem Betreibercomputer (10) über ein Datennetz (NET) verbundene Leseneinrichtung (2) gebildet ist, wobei die Leseeinrichtung (2) die zumindest eine Schnittstelle (12) und zumindest einen Teil der Rechnermittel (13) der Veränderungseinrichtung (5) enthält.

Zusammenfassung:

Erteilungsverfahren zum Erteilen einer Veränderungsberechtigung

Eine Veränderungseinrichtung (5) ist zum Verändern einer von einem Datenträger (S) abgearbeiteten Applikation (A1, A2, A3, A4) ausgebildet, wobei in dem Datenträger (S) eine erste Schlüsselinformation (K1) und in der Veränderungseinrichtung eine zugehörige zweite Schlüsselinformation (K2) gespeichert ist.

(Figur 1)

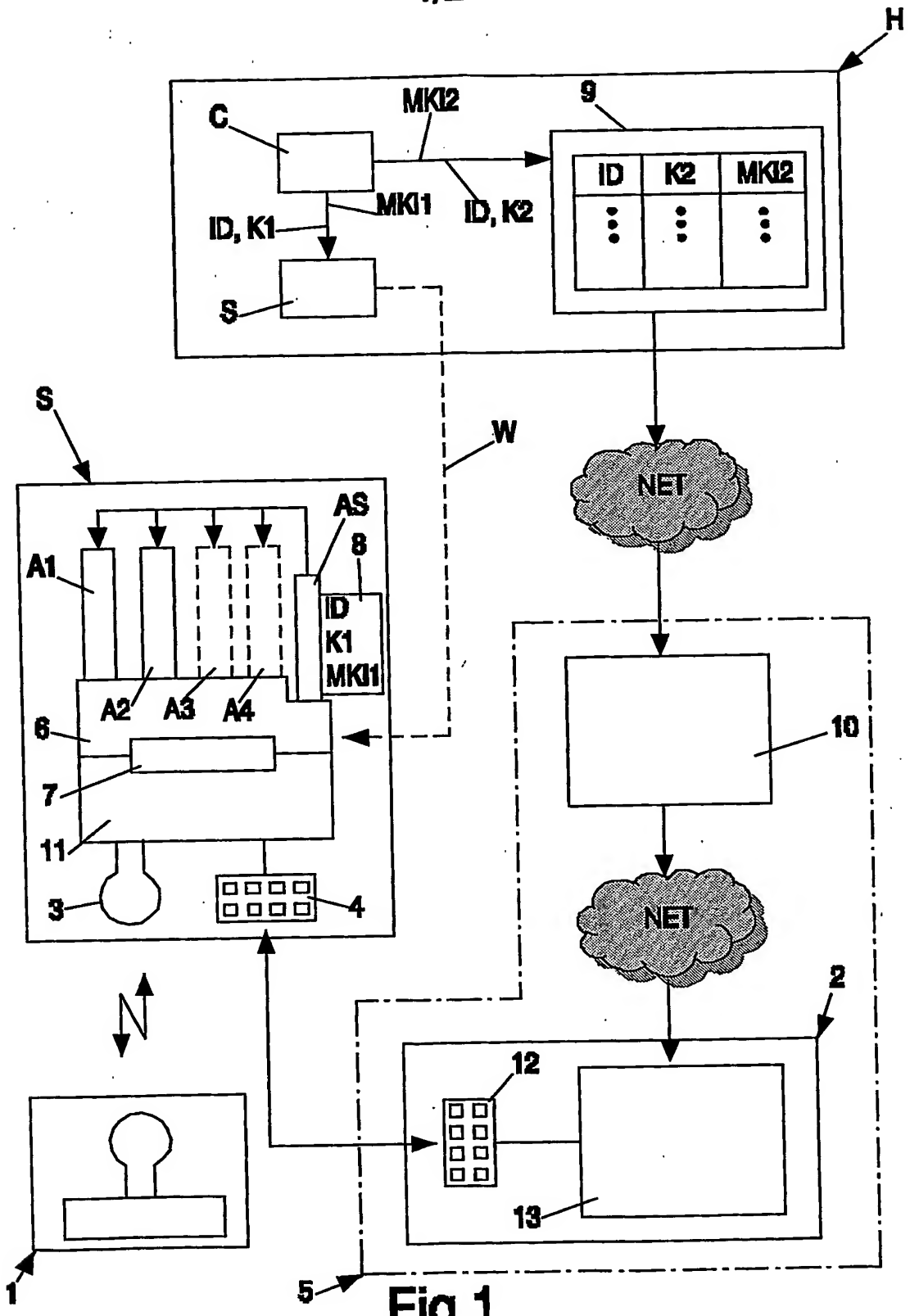
H
C
MKI2
9
ID
K2
MKI2
MKI1
ID, K1
ID, K2
S
W
NET
AS
8
A1
ID
K1
MKI1
A2
A3
A4
6
7
11
3
4
10
NET
2
12
13
1
5

Fig.1

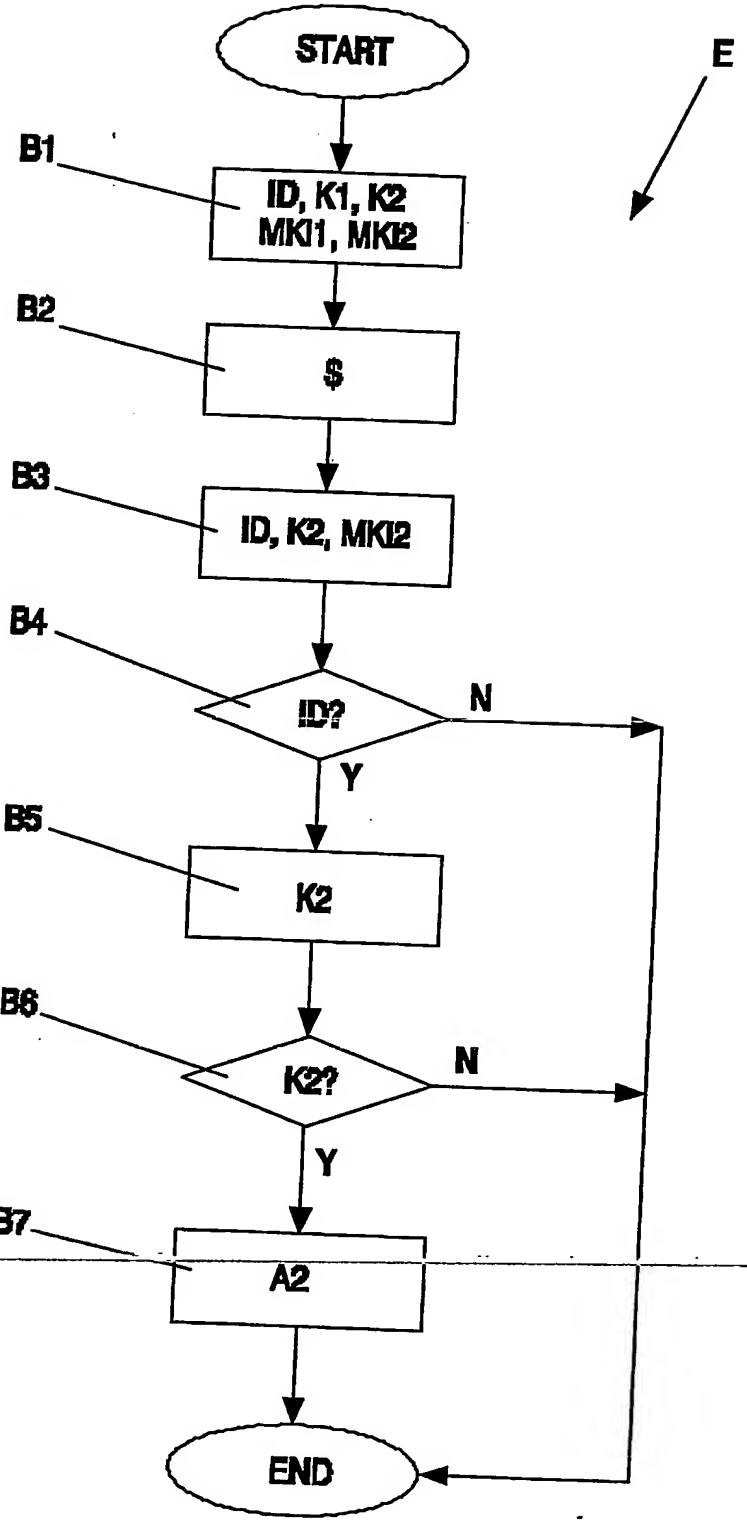
START
E
B1
ID, K1, K2
MK1, MK12
B2
$
B3
ID, K2, MK12
B4
ID?
N
Y
B5
K2
B6
K2?
N
Y
B7
A2
END

Fig.2

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.